

DECOMPOSITIONS OF SINGULAR ABELIAN SURFACES

ROBERTO LAFACE

Dedicated to my father on the occasion of his 50th birthday.

ABSTRACT. Given an abelian surface, the number of its distinct decompositions into a product of elliptic curves has been described by Ma. Moreover, Ma himself classified the possible decompositions for abelian surfaces of Picard number $1 \leq \rho \leq 3$. We explicitly find all such decompositions in the case of abelian surfaces of Picard number $\rho = 4$. This is done by computing the transcendental lattice of products of isogenous elliptic curves with complex multiplication, generalizing a technique of Shioda and Mitani, and by studying the action of a certain class group on the factors of a given decomposition. We also provide an alternative and simpler proof of Ma’s formula, and an application to singular K3 surfaces.

CONTENTS

1. Introduction	1
2. Preliminaries	3
3. Some admissible decompositions	11
4. Explicit computation of transcendental lattices	16
5. Decompositions in the cases $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$	20
6. Decompositions in the remaining cases	26
References	29

1. INTRODUCTION

After the ground breaking work of Shioda and Mitani [10], and of Shioda and Inose [9], singular abelian surfaces, i.e. abelian surfaces of maximum Picard number, have played a key role in the theory of K3 surfaces, because of the rich arithmetic information they carry. This data is encoded in the transcendental lattice, and it naturally transfers to singular K3 surfaces by means of a Shioda-Inose structure [6]. The associated singular K3 surface, which has the same transcendental lattice by a result of Shioda and Inose [9], inherits some of the arithmetic

structure of the associated singular abelian surface. This has been employed, for instance, in the study of the field of definition of singular K3 surfaces by Schütt in [7].

In [5], Ma gives a formula for the number of decompositions of an abelian surface into the product of elliptic curves; this expression is in terms of the arithmetic of the transcendental lattice. The proof builds on lattice theoretical methods, and it works for abelian surfaces of any Picard number. Also, he is able to classify all the distinct decompositions of a given abelian surface of Picard number $\rho \leq 3$. However, there is no mention of the possible decompositions that can appear in the case of singular abelian surfaces. The main purpose of this paper is to classify the possible decompositions into the product of two elliptic curves that a singular abelian surface can admit.

The present paper consists of two parts: in the first one, we develop techniques that allow us to understand the behavior of and to compute the transcendental lattices of products of two CM elliptic curves which are mutually isogenous. We would like to stress that such techniques are of interest on their own, as they provide generalizations of previous results of Shioda and Mitani [10] about the geometry of abelian surfaces, and also of Gauß and Dirichlet in the theory of quadratic forms. The second part of this article is concerned with the problem of classifying all the possible decompositions of a given singular abelian surface, and it is the real motivation behind our studies. In doing so, we have tried to highlight the connection between the geometry of this class of surfaces and the arithmetic of quadratic forms as much as possible.

The starting point of our study is the computation of the transcendental lattice of certain singular abelian surfaces. This will eventually suggest that we look at more general singular abelian surfaces, and, in order to do so, we will need to introduce and study the basic properties of the *generalized Dirichlet composition*, a notion that generalizes the usual Dirichlet composition of quadratic forms. This notion is crucial for fully understanding how to compute transcendental lattices of arbitrary products of two CM elliptic curves which are mutually isogenous. We remark that this extends previous work of Shioda and Mitani [10], where the authors computed the transcendental lattice of very special models of singular abelian surfaces in order to prove the surjectivity of the period map. The conclusion is that computing the transcendental lattice of a singular abelian surface boils down to composing two appropriate quadratic forms by means of the generalized Dirichlet

composition (Proposition 4.3).

Afterwards, we turn to the study of the possible decompositions of a given singular abelian surface A . We distinguish two cases, according to whether the CM field K of A is one among $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, or not. In the latter case, we are able to show that a certain class group acts on the set of decompositions of A , and that this action delivers all possible decompositions of A (Theorem 5.8). We also give a new proof of Ma's formula for the number of possible decompositions. The cases where $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$ are handled separately, according to the number of units in \mathcal{O}_K . In both cases, we give a complete classification of the possible decompositions, and we also provide a formula for their number, again distancing ourselves from Ma's approach.

The paper is organized as follows: in Section 2 we go over all the necessary notions and basic result we need, and afterwards (Section 3) we state Ma's result and make a couple of motivating remarks for what is studied thereafter. In Section 4, we study composition of forms living in different class groups, and we compute explicitly the transcendental lattice of a product abelian surface of Picard rank 4, getting even more candidate decompositions. Finally, Section 5 deals with the problem of distinct decompositions: we show that we have build enough decompositions to match Ma's formula in most cases, and this incidentally leads to a new proof of Ma's formula. Afterwards, in Section 6, we completely solve the classification problem for decompositions in the remaining cases, also providing a new approach to the formula giving their number. We conclude the paper with an application to the field of moduli of singular K3 surfaces, and some open problems, in the hope that they might stimulate future research in this direction.

Acknowledgement. I would like to express my gratitude to my advisor Matthias Schütt for fruitful conversations on the topic, and for a key remark that led to the completion of the paper. I also thank Victor González Alonso and Daniel Loughran for detailed comments and suggestions on earlier drafts of the manuscript.

2. PRELIMINARIES

2.1. Singular abelian surfaces. We introduce briefly the basic theory of singular abelian surfaces; for a reference, the reader may see [10]. We will be working over the field of complex numbers. If X is a smooth algebraic surface, we can define the Néron-Severi lattice of X : it is the

group of divisors on X , modulo algebraic equivalence, namely

$$\mathrm{NS}(X) := \mathrm{Div}(X) / \sim_{\mathrm{alg}},$$

together with restriction of the intersection form on $\mathrm{H}^2(X, \mathbb{Z})$. Its rank $\rho(X) := \mathrm{rank} \, \mathrm{NS}(X)$ is called *Picard number* of X ; the Picard number measures how many different curves lie on a surface. By the Lefschetz theorem on $(1, 1)$ -classes, we have the bound

$$\rho(X) \leq h^{1,1}(X) = b_2(X) - 2p_g(X),$$

where $b_2(X) := \mathrm{rank} \, \mathrm{H}^2(X, \mathbb{Z})$ and $p_g(X) := \dim_{\mathbb{C}} \mathrm{H}^0(X, \omega_X)$.

We can consider the lattice

$$\mathrm{H}^2(X, \mathbb{Z})_{\mathrm{free}} := \mathrm{H}^2(X, \mathbb{Z}) / (\text{torsion}),$$

and since $\mathrm{NS}(X) \subset \mathrm{H}^2(X, \mathbb{Z})$, also $\mathrm{NS}(X)_{\mathrm{free}} \subset \mathrm{H}^2(X, \mathbb{Z})_{\mathrm{free}}$; the lattice $\mathrm{NS}(X)_{\mathrm{free}}$ has signature $(1, \rho(X) - 1)$. Its orthogonal complement $\mathrm{T}(X) \subset \mathrm{H}^2(X, \mathbb{Z})_{\mathrm{free}}$ is called the *transcendental lattice* of X , and it has signature

$$(2p_g(X), h^{1,1}(X) - \rho(X)).$$

A smooth algebraic surface with maximum Picard number, i.e. $\rho(X) = h^{1,1}(X)$, is called a *singular surface*. In this case, the transcendental lattice acquires the structure of a positive definite lattice of rank $2p_g(X)$. Throughout the paper, we are going to consider a special class of surfaces, namely singular abelian surfaces. Letting A be such a surface, $\rho(A) = 4$ and $\mathrm{T}(A)$ is a positive definite integral binary form.

We now recall the structure of the period map of an abelian surface A (not necessarily singular). The exponential sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_A \longrightarrow \mathcal{O}_A^\times \longrightarrow 0$$

yields a long exact sequence in cohomology, from which we can extract a map

$$p_A : \mathrm{H}^2(A, \mathbb{Z}) \longrightarrow \mathrm{H}^2(A, \mathcal{O}_A) \cong \mathbb{C},$$

since $p_g(A) = 1$; the map p_A is called *the period map of A* . By using the structure of complex torus of A , we make this more explicit: since

$$\mathrm{H}^2(A, \mathbb{Z}) \cong \bigwedge^2 \mathrm{H}^1(A, \mathbb{Z}) \quad \text{and} \quad \mathrm{H}^1(A, \mathbb{Z}) = \mathrm{H}_1(A, \mathbb{Z})^\vee,$$

we can take a basis $\{v_1, v_2, v_3, v_4\}$ of $\mathrm{H}_1(A, \mathbb{Z})$ and the corresponding dual basis $\{u^1, u^2, u^3, u^4\}$. Then, setting $u^{ij} := u^i \wedge u^j$, we get a basis of $\mathrm{H}^2(A, \mathbb{Z})$ by considering

$$\{u^{ij} \mid 1 \leq i < j \leq 4\},$$

which also gives a basis of $H^2(A, \mathbb{C})$. As an element of $H^2(A, \mathbb{C}) \cong \text{Hom}(H^2(A, \mathbb{Z}), \mathbb{C})$ (here we tacitly use Poincaré duality), the period map has the following description:

$$p_A = \sum_{i < j} \det(v_i | v_j) u^{ij},$$

where the notation $(v_i | v_j)$ indicates the matrix whose columns are v_i and v_j . Notice that, since $\text{NS}(A) = \ker(p_A)$ and $T(A) = (\ker(p_A))^\perp$, this allows us to explicitly compute the Néron-Severi and the transcendental lattices. Also, the period map satisfies the period relations

$$(p_A, p_A) = 0 \quad \text{and} \quad (p_A, \overline{p_A}) > 0.$$

2.2. Class group theory. We recall a few facts on integral binary quadratic forms; for a detailed account, the reader is suggested to see [2]. Given a form

$$Q(x, y) = ax^2 + bxy + cy^2$$

the quantity $\gcd(a, b, c)$ is called *index of primitivity* and Q is said *primitive* if $\gcd(a, b, c) = 1$. Sometimes, it is convenient to extract the *primitive part* of a form Q : this is the quadratic form Q_0 such that $mQ_0 = Q$, m being the index of primitivity of Q . A form Q represents $m \in \mathbb{Z}$ if $m = Q(x, y)$ for some $x, y \in \mathbb{Z}$; if moreover $\gcd(x, y) = 1$, then we say that Q properly represents $m \in \mathbb{Z}$. A quadratic form Q as above will be denoted in short by $Q = (a, b, c)$. Two forms $Q = (a, b, c)$ and $Q' = (a', b', c')$ are equivalent (properly equivalent, respectively) if there exists $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ ($\text{SL}_2(\mathbb{Z})$, respectively) such that

$$Q(px + qy, rx + sy) = Q'(x, y).$$

The following basic results give a hint on why it is important to know which numbers a form represents.

Lemma 2.1 (Lemma 2.3 in [2]). *A form Q properly represents $m \in \mathbb{Z}$ if and only if Q is properly equivalent to the form (m, B, C) , for some $B, C \in \mathbb{Z}$.*

Lemma 2.2 (Lemma 2.25 in [2]). *Given a form Q and an integer M , Q represents infinitely many numbers prime to M .*

The *discriminant* of a form $Q = (a, b, c)$ is the integer $D := b^2 - 4ac$. The set of proper equivalence classes of primitive forms of discriminant D is called the *(form) class group of discriminant D* , and it is denoted by $C(D)$; we will denote the class of a form Q by $[Q]$. The class group is equipped with the Dirichlet composition of forms: by [2, Lemma 3.2],

if $Q = (a, b, c)$ and $Q' = (a', b', c')$ are primitive forms of discriminant D , such that

$$\gcd\left(a, a', \frac{b+b'}{2}\right) = 1,$$

then the composition $Q * Q'$ is the form (aa', B, C) , where $C = \frac{B^2 - D}{4aa'}$ and B is the integer, unique modulo $2aa'$, such that

$$\begin{cases} B \equiv b \pmod{2a}, \\ B \equiv b' \pmod{2a'}, \\ B^2 \equiv D \pmod{4aa'}. \end{cases}$$

Naturally, we put $[Q] * [Q'] := [Q * Q']$. Notice that the arithmetic properties of B allow us to rewrite $\tau(Q)$ and $\tau(Q')$: indeed, we can always assume that

$$\tau(Q) = \frac{-B + \sqrt{D}}{2a}, \quad \tau(Q') = \frac{-B + \sqrt{D}}{2a'},$$

and furthermore $\gcd(a, a', \frac{b+b'}{2}) = 1$.

Recall that, fixed a quadratic imaginary field K , an order \mathcal{O} is a subring of K containing the unity of K which has also the structure of a rank-two free \mathbb{Z} -module. Every order \mathcal{O} can be written in a unique way as

$$\mathcal{O} = \mathbb{Z} + fw_K\mathbb{Z}, \quad w_K := \frac{d_K + \sqrt{d_K}}{2}, \quad d_K := \text{disc } \mathcal{O}_K, \quad f \in \mathbb{Z}^+.$$

The integer f is called the *conductor* of \mathcal{O} , and it characterizes \mathcal{O} in a unique way; we will denote the order of conductor f in \mathcal{O}_K by $\mathcal{O}_{K,f}$. Similarly, a *module* M in K is a rank-two \mathbb{Z} -submodule of K (no condition on the unity). Two modules M_1 and M_2 are equivalent ($M_1 \sim M_2$) if they are homothetic, i.e. there exists $\lambda \in K$ such that $\lambda M_1 = M_2$. To any module M , we can associate its *complex multiplication* (CM) *ring*¹

$$\mathcal{O}_M := \{x \in K \mid xM \subseteq M\}.$$

Notice that \mathcal{O}_M is an order in K , and that equivalent modules in K have the same CM ring. The product module M_1M_2 is defined in a natural way, and if f_i is the conductor of M_i ($i = 1, 2$), then $\mathcal{O}_{M_1M_2} = \mathcal{O}_{K,(f_1, f_2)}$, the latter being the order of conductor (f_1, f_2) in K .

For an order \mathcal{O} in a quadratic field K , it is possible to define a class group $C(\mathcal{O})$: letting $I(\mathcal{O})$ denote the group of proper fractional ideals,

¹The name CM ring refers to the property $\mathcal{O}_M = \text{End}(\mathbb{C}/M)$.

meaning those whose CM ring is \mathcal{O} itself, and letting $P(\mathcal{O})$ be the subgroup generated by the principal ones, we set $C(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$, and we call it the *ideal class group* of \mathcal{O} . An important result in algebraic number theory states that if $\text{disc } \mathcal{O} = D$, then $C(D) \cong C(\mathcal{O})$. From now on, we will use interchangeably the two class groups to our convenience. The order of the class group $C(\mathcal{O})$ is called the *class number* of \mathcal{O} , and it is denoted by $h(\mathcal{O}_{K,f})$, or $h(D)$ according to the isomorphism between form and ideal class group. There is a beautiful formula that describes the order of the class group of an order in terms of its conductor and the maximal order that contains it.

Theorem 2.3 (Theorem 7.24 in [2]). *Let $\mathcal{O}_{K,f}$ be the order of conductor f in \mathcal{O}_K . Then*

$$h(\mathcal{O}_{K,f}) = \frac{h(\mathcal{O}_K) \cdot f}{[\mathcal{O}_K^\times : \mathcal{O}_{K,f}^\times]} \prod_{p|f} \left(1 - \left(\frac{d_K}{p} \right) \frac{1}{p} \right),$$

where p runs over the primes dividing the conductor f .

2.3. The moduli space of singular abelian surfaces. Let Σ^{Ab} be the moduli space of singular abelian surfaces². In [10], Shioda and Mi-tani described Σ^{Ab} by means of the transcendental lattice $T(A)$ associated to any singular abelian surface A . We say that $T(A)$ is *positively oriented* if

$$T(A) = \mathbb{Z}\langle t_1, t_2 \rangle \quad \text{and} \quad \text{Im}(p_A(t_1)/p_A(t_2)) > 0.$$

Notice that the transcendental lattice $T(A)$ is an even lattice $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$, and thus we can always associate to it the quadratic form (a, b, c) . This realizes a 1:1 correspondence, and therefore we can naturally see the transcendental lattice as an integral binary quadratic form. We can associate to any quadratic form $Q = (a, b, c)$ an abelian surface A_Q . In order to describe the correspondence, we set

$$\tau \equiv \tau(Q) := \frac{-b + \sqrt{D}}{2a}, \quad D := \text{disc } Q = b^2 - 4ac,$$

and we will denote by E_τ the elliptic curve \mathbb{C}/Λ_τ , Λ_τ being the lattice $\mathbb{Z} + \tau\mathbb{Z}$. The abelian surface associated to a form Q is then defined as the product surface

$$A_Q := E_\tau \times E_{a\tau+b}.$$

²By moduli space, we do not mean the solution to a moduli problem, but rather the set of isomorphism classes of singular abelian surfaces

The mapping $Q \mapsto A_Q$ realizes a 1:1 correspondence between $\mathrm{SL}_2(\mathbb{Z})$ -conjugacy classes of binary forms and isomorphism classes of singular abelian surfaces, namely

$$\Sigma^{\mathrm{Ab}} \longleftrightarrow \mathcal{Q}^+ / \mathrm{SL}_2(\mathbb{Z}),$$

\mathcal{Q}^+ being the set of positive definite integral binary quadratic forms. By dropping the orientation, we get a 2:1 map $\Sigma^{\mathrm{Ab}} \rightarrow \mathcal{Q}^+ / \mathrm{GL}_2(\mathbb{Z})$, which is just taking the transcendental lattice of an abelian surface:

$$\Sigma^{\mathrm{Ab}} \ni [A] \longmapsto [\mathrm{T}(A)] \in \mathrm{GL}_2(\mathbb{Z}).$$

As a consequence, we get that every singular abelian surface A is isomorphic to the product of two isogenous elliptic curves with complex multiplication. Therefore, we can ask the following

Question 2.4.

1. Given a singular abelian surface A , how many distinct decompositions of A into the product of two elliptic curves are there?
2. Can we list all the possible decompositions?

Part 1 has been completely solved by Ma [5], for abelian surfaces of any Picard number. Concerning Part 2, in case $\mathrm{T}(A) = Q$, for a primitive form Q , the answer is given in [10, Theorem 4.7], and the formula depends on the structure of the class group of a certain order. We don't discuss this any further here, because, for our purposes, we will need a different, and somehow easier, interpretation of this result, which will be given in Lemma 3.2.

2.4. Class field theory. For later reference, we need to state a couple of facts from class field theory; see [2] for an account on the subject. Let K be a number field, and let \mathfrak{m} be a *modulus* in K , i.e. a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

over all primes \mathfrak{p} of K , finite or infinite, where the exponents satisfy

- (1) $n_{\mathfrak{p}} \geq 0$, and at most finitely many are nonzero;
- (2) $n_{\mathfrak{p}} = 0$, for \mathfrak{p} a complex infinite prime;
- (3) $n_{\mathfrak{p}} \leq 1$, for \mathfrak{p} a real infinite prime.

Consequently, any modulus \mathfrak{m} can be written as $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_{\infty}$, where \mathfrak{m}_0 is an \mathcal{O}_K -ideal and \mathfrak{m}_{∞} is a product of distinct real infinite primes of K . We define $I_K(\mathfrak{m})$ to be the group of fractional ideals of K that are coprime to \mathfrak{m} , and we let $P_{K,1}(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ generated by the principal ideals $\alpha \mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies

$$\alpha \equiv 1 \pmod{\mathfrak{m}_0}, \quad \sigma(\alpha) > 0 \text{ for every real infinite prime } \sigma | \mathfrak{m}_{\infty}.$$

One sees that $P_{K,1}(\mathfrak{m})$ is of finite index in $I_K(\mathfrak{m})$. A subgroup $H \subseteq I_K(\mathfrak{m})$ is called a *congruence subgroup* for \mathfrak{m} if

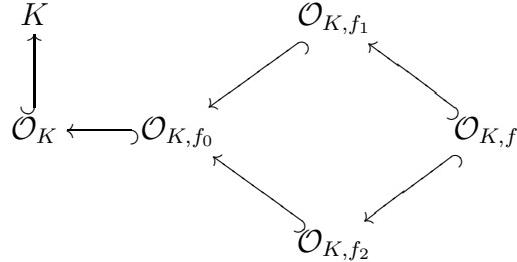
$$P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m}),$$

and the quotient $I_K(\mathfrak{m})/H$ is called a *generalized class group* of \mathfrak{m} . Let now L be an abelian extension of K , and assume that \mathfrak{m} is divisible by all primes of K that ramify in L . Then, for a given prime \mathfrak{p} in K , one can define the Frobenius element associated to \mathfrak{p} by means of the Artin symbol $(\frac{L/K}{\mathfrak{p}}) \in \text{Gal}(L/K)$, thus defining a map

$$\Phi_{\mathfrak{m}}^{L/K} : I_K(\mathfrak{m}) \longrightarrow \text{Gal}(L/K),$$

called the *Artin map* for L/K and \mathfrak{m} .

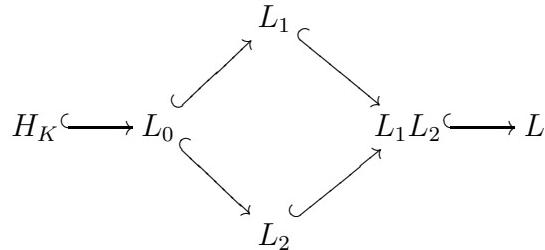
Suppose we have the diagrams of orders



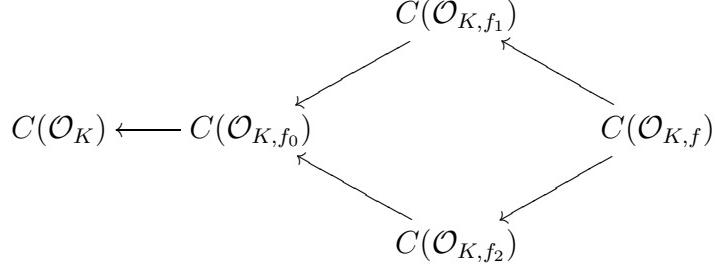
where $f_1, f_2 \geq 1$, $f_0 = \gcd(f_1, f_2)$ and $f = \text{lcm}(f_1, f_2)$. Let $i = 0, 1, 2, \emptyset$; since

$$P_{K,1}(f_i \mathcal{O}_K) \subseteq P_{K,\mathbb{Z}}(f_i) \subseteq I_K(f_i) = I_K(f_i \mathcal{O}_K),$$

by the Existence Theorem, there exists a unique abelian extension L_i/K all of whose ramified primes divide $f_i \mathcal{O}_K$, such that $\ker(\Phi_{f_i \mathcal{O}_K}^{L_i/K}) = P_{K,\mathbb{Z}}(f_i)$, i.e. $\text{Gal}(L_i/K) \cong C(\mathcal{O}_{K,f_i})$. This extension is called the *ring class field* of \mathcal{O}_{K,f_i} ; at the level of ring class fields, we get induced a diagram of field extensions.



By Galois theory, we get the following induced diagram of class groups.



In most cases the field L is precisely the composite of L_1 and L_2 , as it is stated in the following

Proposition 2.5 (Proposition 3.1 in [1]). *Assume all conditions above are satisfied.*

- (1) *If $d_K \neq -3, -4$, then $L = L_1L_2$.*
- (2) *Assume $d_K \in \{-3, -4\}$.*
 - (a) *If f_1 or f_2 is equal to 1, or $f_0 > 1$, then $L = L_1L_2$.*
 - (b) *If $f_1, f_2 > 1$ and $f_0 = 1$, then $L_1L_2 \subsetneq L$; moreover, the extension L/L_1L_2 has degree 2 if $d_K = -4$, and degree 3 if $d_K = -3$.*

2.5. Numbers represented by the principal form. For two sets S and T , we say that $S \dot{\subset} T$ if $S \subseteq T \cup \Sigma$, where Σ is a finite set; analogously, $S \doteq T$ means that both $S \dot{\subset} T$ and $T \dot{\subset} S$ hold. Suppose we are now given a quadratic form Q ; then, we can ask about the primes represented by Q , i.e. about the set

$$\mathcal{P}_Q := \{p \text{ prime} \mid p \text{ is represented by } Q\}.$$

It turns out that

$$\mathcal{P}_Q \doteq \left\{ p \text{ prime} \mid p \text{ unramified in } K, \left(\frac{L/K}{p} \right) = \langle \sigma \rangle \right\} =: \hat{\mathcal{P}}_Q,$$

where $\langle \sigma \rangle$ is the conjugacy class of the element $\sigma \in \text{Gal}(L/K)$ corresponding to the ideal associated to the form Q , K is the quadratic imaginary field of discriminant $\text{disc } Q$, and L is the ring class field of the order \mathcal{O} of discriminant $\text{disc } Q$. Notice that in case $Q = P$, the principal form, then $\hat{\mathcal{P}}_P = \text{Spl}(L/\mathbb{Q})$, $\text{Spl}(L/\mathbb{Q})$ being the set of primes in \mathbb{Q} that split completely in L . For later reference, we mention the following

Lemma 2.6 (Exercise 8.14 in [2]). *Let L and M be two finite extensions of K , and let \mathcal{P} be a prime in K that splits completely in both L and M ; then \mathcal{P} splits completely in the composite LM . Consequently, $\text{Spl}(LM/K) = \text{Spl}(L/K) \cap \text{Spl}(M/K)$.*

3. SOME ADMISSIBLE DECOMPOSITIONS

3.1. Number of decompositions. In [5], Ma solves the problem of finding the number of distinct decompositions of an abelian surface. The techniques he employs are lattice theoretical, and the formulas strongly depend on the arithmetic of the transcendental lattice. However, no explicit decomposition is exhibited for singular abelian surfaces.

We briefly recall Ma's results for an abelian surface A with Picard number $\rho(A) = 4$. Such a surface is necessarily the product of two isogenous elliptic curves E_1, E_2 with complex multiplication. Following [5], if $A \cong E_1 \times E_2$, then we say that the decomposition (E_1, E_2) is *admissible*. Two decompositions (E_1, E_2) and (F_1, F_2) of A are *isomorphic* if $E_1 \cong F_1$ and $E_2 \cong F_2$, or $E_1 \cong F_2$ and $E_2 \cong F_1$, and analogously, two decompositions (E_1, E_2) and (F_1, F_2) of A are *strictly isomorphic* if $E_1 \cong F_1$ and $E_2 \cong F_2$. Let $\text{Dec}(A)$ be the set of isomorphism classes of decompositions of A , and similarly let $\widetilde{\text{Dec}}(A)$ be the set of strict isomorphism classes of decompositions of A . Also, define

$$\delta(A) := \#\text{Dec}(A), \quad \widetilde{\delta}(A) := \#\widetilde{\text{Dec}}(A).$$

To relate $\delta(A)$ and $\widetilde{\delta}(A)$, we consider the number of decompositions into the self-product of an elliptic curve. To this end, we define

$$\delta_0(A) := \#(\{E \text{ elliptic curve} : A \cong E \times E\} / \cong),$$

and we have the obvious relation

$$\widetilde{\delta}(A) = 2\delta(A) - \delta_0(A).$$

For $n > 1$, let $\tau(n)$ be the number prime factors of n , and set $\tau(1) = 1$. Moreover, for a quadratic form Q , let $g(Q)$ denote its genus, i.e. the set of isometry classes of lattices isogenous to Q , and let $\widetilde{g}(Q)$ denote its proper genus, i.e. the set of isometry classes of oriented lattices isogenous to Q . Then we have the following result

Theorem 3.1 (Theorem 1.2, Theorem 1.3, Example 5.13 in [5]). *Let A be an abelian surface of Picard number $\rho(A) = 4$.*

- (1) *If $T(A)$ is not isometric to $\begin{pmatrix} 2n & 0 \\ 0 & 2n \end{pmatrix}$ or $\begin{pmatrix} 2n & n \\ n & 2n \end{pmatrix}$, $n > 1$, one has*

$$\delta(A) = \sum_{T \in g(T(A))} \#(O(A_T)/O(T)), \quad \widetilde{\delta}(A) = 2^{-1} \cdot \#\widetilde{g}(T(A)) \cdot \#O(A_{T(A)}).$$

(2) If $T(A) \cong \begin{pmatrix} 2n & 0 \\ 0 & 2n \end{pmatrix}$, then

$$\delta(A) = (2^{-4} + 2^{-\tau(n)-3}) \cdot \#O(A_{T(A)}), \quad \tilde{\delta}(A) = 2\delta(A).$$

(3) If $T(A) \cong \begin{pmatrix} 2n & n \\ n & 2n \end{pmatrix}$, then

$$\delta(A) = \begin{cases} 3^{-2} \cdot (2^{-2} + 2^{-\tau(n)}) \cdot \#O(A_{T(A)}) & n \text{ odd} \\ 3^{-2} \cdot (2^{-2} + 2^{-\tau(2^{-1}n)}) \cdot \#O(A_{T(A)}) & n \text{ even} \end{cases}, \quad \tilde{\delta}(A) = 2\delta(A).$$

(4) If $T(A)$ is either $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ or $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, then $\delta(A) = \delta_0(A) = \tilde{\delta}(A) = 1$.

Under the assumption that $T(A)$ is primitive, Shioda and Mitani [10, Theorem 4.7] proved a formula for the number of decompositions which depended only on the structure of a certain class group. In [5], the aforementioned formula is given the following interpretation

Corollary 3.2 (Corollary 5.11 in [5]). *Let A be a singular abelian surface having primitive transcendental lattice $T(A)$, and let $D := -\det T(A) < 0$. Then, $\tilde{\delta}(A) = h(D)$.*

Concerning the study of singular abelian surfaces with imprimitive transcendental lattice $T(A)$, Ma [5] gives an analogous formula for $T(A)$ not isometric to $\begin{pmatrix} 2n & 0 \\ 0 & 2n \end{pmatrix}$ or $\begin{pmatrix} 2n & n \\ n & 2n \end{pmatrix}$, $n > 1$.

Corollary 3.3 (Corollary 5.12 in [5]). *Let A be a singular abelian surface having primitive transcendental lattice $T(A)$, and let $D := -\det T(A) < 0$. Let A_n be the singular abelian surface of transcendental lattice $n \cdot T(A) := T(A)[n]$. If $\det T(A) \neq 3, 4$, then $\tilde{\delta}(A_n) = 2^{\tau(n)} \cdot h(n^2 D)$.*

3.2. Some explicit decompositions. We now explain how to obtain a first type of decompositions, which are related to the primitive part of the transcendental lattice. The idea comes from [10], in particular their explicit description of the period map for singular abelian surfaces. Notice that Shioda and Mitani gave a method to construct a singular abelian surface A_Q of transcendental lattice $T(A) = Q$. Although the idea is the same, at some point we will need some number theoretical statement from class group theory, crucial for our computations.

We now briefly explain where we got the idea from. In [10], there is given a criterion to establish whether a certain decomposition is admissible. If A has transcendental lattice $Q = mQ_0$, with Q_0 primitive, let

$$M_0 := Z + \tau(Q)\mathbb{Z} = \mathbb{Z} + \tau(Q_0)\mathbb{Z},$$

and let f_0 be the conductor of its CM ring

$$\mathcal{O}_{\mathbb{Z} + \tau(Q)\mathbb{Z}} = \mathbb{Z} + \frac{-b_0 + \sqrt{D_0}}{2}\mathbb{Z}.$$

Proposition 3.4 (Proposition 4.5 in [10]). *Let A_Q be the abelian surface associated to the quadratic form Q , and let M_i be the module of conductor f_i in $K = \mathbb{Q}(\tau(Q))$, $i = 1, 2$. Then $A \cong \mathbb{C}/M_1 \times \mathbb{C}/M_2$ if and only if $M_1 M_2 \sim M_0$, $(f_1, f_2) = f_0$ and $f_1 f_2 = m f_0^2$.*

From this result, we now deduce some necessary conditions for a decomposition to be admissible. From the last two properties, it follows that $\bar{f}_1 := f_1/f_0$ and $\bar{f}_2 := f_2/f_0$ are relatively prime, and hence we find a first upper bound to the number of decompositions (absolutely not sharp, since we haven't used one of the conditions in [10, Proposition 4.5]). In fact, f_0 is uniquely determined by Q , and thus the only choice we have is about \bar{f}_1 and \bar{f}_2 , which have to satisfy $(\bar{f}_1, \bar{f}_2) = 1$ and $n = \bar{f}_1 \bar{f}_2$. The number of choices of pairs (\bar{f}_1, \bar{f}_2) with $\gcd(\bar{f}_1, \bar{f}_2) = 1$ is indeed $2^{\tau(n)}$, and f_1 (f_2 , respectively) determines univocally the order of conductor f_1 (f_2 , respectively), thus

$$\tilde{\delta}(A) \leq \sum_{\substack{\bar{f}_1 \bar{f}_2 = n \\ (\bar{f}_1, \bar{f}_2) = 1}} h(\mathcal{O}_{K, f_1}) h(\mathcal{O}_{K, f_2}) \leq 2^{\tau(n)} h(\mathcal{O}_{K, n})^2.$$

Notice that, if $Q = nQ_0$, then

$$A_Q := E_{\tau(Q_0)} \times E_{\tau(P)} = E_{\tau(Q_0)} \times E_{n\tau(P_0)},$$

where P is the principal form of discriminant $D = \text{disc } Q$, and P_0 is the principal form of discriminant $D_0 = D/n^2$; also, $T(A) = nQ_0 = n(Q_0 * P_0)$. This motivates the study of the transcendental lattice of $E_{\tau(Q_0)} \times E_{n\tau(P_0)}$, where $Q_0, P_0 \in C(D/n^2)$, which incidentally gives examples of decompositions coming from pairs $(\bar{f}_1, \bar{f}_2) = (1, n)$. More generally, we will be interested in abelian surfaces of the form

$$E_{s\tau(Q_0)} \times E_{t\tau(P_0)},$$

where $st = n$. Under the assumption $\gcd(s, t) = 1$, we are able to compute the transcendental lattice of this class of surfaces.

Proposition 3.5. *Let $[Q] = s[Q_0]$, $[Q'] = t[Q'_0]$ be such that $[Q_0], [Q'_0] \in C(D_0)$, for some $D_0 < 0$, and suppose $\gcd(s, t) = 1$. Then*

$$[\mathrm{T}(E_{s\tau(Q_0)} \times E_{t\tau(Q'_0)})] = st[Q_0 * Q'_0].$$

Proof. Let

$$\tau_1 := s \frac{-b_0 + \sqrt{D_0}}{2a_0}, \quad \tau_2 := t \frac{-b'_0 + \sqrt{D_0}}{2a'_0}.$$

Now, let B_0 be the element described in [2, Lemma 3.2]; by virtue of these relations (together with $\mathrm{SL}_2(\mathbb{Z})$ -invariance of the j -invariant), we can replace b_0 and b'_0 by B_0 without changing the isomorphism classes of the elliptic curves. Therefore, we can assume that

$$\tau_1 = s \frac{-B_0 + \sqrt{D_0}}{2a_0}, \quad \tau_2 = s \frac{-B_0 + \sqrt{D_0}}{2a'_0}.$$

By [10],

$$p_A = u^{12} + \tau_2 u^{14} + \tau_1 u^{23} - \tau_1 \tau_2 u^{34},$$

and $\mathrm{NS}(A) = \ker(p_A)$. By picking an element

$$v = \sum_{1 \leq i < j \leq 4} A_{ij} u^{ij} \in \mathrm{NS}(A)_{\mathbb{Q}},$$

and looking at its image under the period map, we see that

$$\begin{aligned} 0 = p_A(v) = & \left[A_{34} - \frac{tB_0}{2a'_0} A_{23} - \frac{sB_0}{2a_0} A_{14} - st \frac{D_0 + B_0^2}{4a_0 a'_0} A_{12} \right] + \\ & + \sqrt{D_0} \left[\frac{t}{2a'_0} A_{23} + \frac{s}{2a_0} A_{14} + st \frac{B_0}{2a_0 a'_0} A_{12} \right]. \end{aligned}$$

Solving the system of equations given by the pair of brackets, we get

$$A_{23} = -\frac{s}{a_0 t} (a'_0 A_{14} + t B_0 A_{12}), \quad A_{34} = st \frac{D_0 - B_0^2}{4a_0 a'_0} A_{12},$$

which in turn give an explicit description of

$$\mathrm{NS}(A)_{\mathbb{Q}} = \mathbb{Q} \left\langle u^{12} - \frac{sB_0}{a_0} u^{23} + std_0 u^{34}, u^{13}, u^{24}, u^{14} - \frac{sa'_0}{ta_0} u^{23} \right\rangle,$$

$$\text{with } d_0 := \frac{D_0 - B_0^2}{4a_0 a'_0}.$$

Now we want to compute $\mathrm{T}(A) = \mathrm{NS}(A)^{\perp}$: let

$$v = \sum_{1 \leq i < j \leq 4} A_{ij} u^{ij} \in \mathrm{NS}(A)^{\perp} = \mathrm{NS}(A)_{\mathbb{Q}}^{\perp},$$

and consider the relations coming by intersecting the generators of $\mathrm{NS}(A)_{\mathbb{Q}}$ with v .

$$A_{24} = 0 \quad (1)$$

$$A_{13} = 0 \quad (2)$$

$$A_{34} - \frac{sB_0}{a_0} A_{14} + std_0 A_{12} = 0 \quad (3)$$

$$A_{23} - \frac{sa'_0}{ta_0} A_{14} = 0 \quad (4)$$

Equations (1) and (2) give clear conditions on the coefficients of v . Turning to (3) and (4), we can assume that $(a_0, a'_0) = (a_0, s) = 1$ by [2, Lemmata 2.3 and 2.25]; furthermore, we can assume $t \nmid a'_0$. Under these hypotheses, equation (4) yields

$$A_{14} = a_0 A'_{14} = a_0 t A''_{14}, \quad A_{23} = sa'_0 A''_{14},$$

and therefore we get

$$A_{34} = stB_0 A''_{14} - std_0 A_{12}$$

from equation (3). This leads to two generators for $\mathrm{T}(A)$, namely

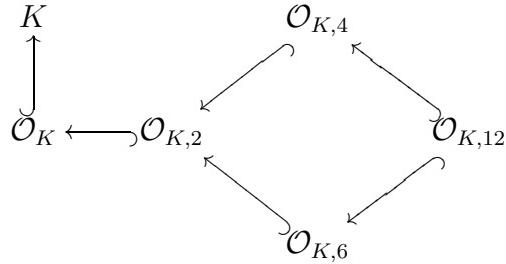
$$\mathrm{T}(A) = \mathbb{Z} \left\langle a_0 tu^{14} + sa'_0 u^{23} + stB_0 u^{34}, u^{12} - std_0 u^{34} \right\rangle.$$

The intersection matrix of $\mathrm{T}(A)$ is shown to be $st \begin{pmatrix} 2a_0 a'_0 & B_0 \\ B_0 & -2d_0 \end{pmatrix}$, and one can easily check that the matrix is (positively) oriented. \square

If A is a singular abelian surface of transcendental lattice $Q = nQ_0$, we get $2^{\tau(n)} h(D/n^2)$ decompositions of A , $D = -\det \mathrm{T}(A)$.

Corollary 3.6. *If $\mathrm{T}(A) = Q = nQ_0$, then we get decompositions of A as $E_{s\tau(Q_0 * R_0)} \times E_{t\tau(R_0^{-1} * Q_0)}$, for $R_0 \in C(\mathrm{disc} Q_0)$, $n = st$, $(s, t) = 1$.*

Example 3.7. Let A have transcendental lattice $6(1, 0, 3) \in \overline{C}(-432)$. Proposition 3.4 tell us that, in order to find all decompositions of A , we must inspect the folowing orders.



According to Corollary 3.3, the number of strict decompositions is $\tilde{\delta}(A) = 24$, while Corollary 3.6 allows us to retrieve only 4 of those. This happens because we only considered elliptic curves with CM by $\mathcal{O}_{K,2}$ and $\mathcal{O}_{K,12}$. \square

The example shows that, in order to being able to exhibit all decompositions, we need to compute the transcendental lattice of the product of elliptic curves with CM by $\mathcal{O}_{K,4}$ and $\mathcal{O}_{K,3}$. The proof of Theorem 3.5 suggests that this would be possible if we were able to compose forms from different class groups.

4. EXPLICIT COMPUTATION OF TRANSCENDENTAL LATTICES

4.1. Composition between different class groups. The idea behind Dirichlet composition is that two forms $f(x, y)$ and $g(x, y)$ (having the same discriminant D) give rise to a new form $F(x, y)$ (again of discriminant D) with the property

$$f(x, y) \cdot g(x, y) = F(B_1(x, y, z, w), B_2(x, y, z, w)),$$

for $B_i(x, y, z, w) \in \mathbb{Z}[xz, xw, yz, yw]$. In particular, the product of numbers represented by $f(x, y)$ and $g(x, y)$ are represented by $F(x, y)$.

If $f(x, y)$ and $g(x, y)$ are not of the same discriminant, we can multiply them by a positive integer to obtain two new forms having the same discriminant. Namely, given $Q_0 \in C(D_0)$ and $Q'_0 \in C(D'_0)$, with $D_0 = f_0^2 d_K$ and $D'_0 = f'_0^2 d_K$, set $f := \text{lcm}(f_0, f'_0)$. Then, putting

$$D := f^2 d_K, \quad d := f/f_0, \quad d' := f/f'_0,$$

the forms $Q := dQ_0$ and $Q' := d'Q'_0$ have discriminant D ; we get two classes in the *extended class group*³

$$\overline{C}(D) := \bigsqcup_{m|f(D)} m \cdot C(D/m^2),$$

namely $[Q] := d[Q_0]$ and $[Q'] := d'[Q'_0]$, and thus we can use Dirichlet composition after considering a suitable representative. Since d and d' are coprime, $Q = (a, b, c)$ and $Q' = (a', b', c')$ can be assumed to have coprime leading coefficients, hence we do have a composition: it is defined as usual (see [2, Theorem 3.8]), and it extends to elements of the (extended) class group.

³The name is actually misleading since this is not a group.

Lemma 4.1. *Assume that $Q = (a, b, c)$ and $Q' = (a', b', c')$ are primitive, and suppose that*

$$n^2 \operatorname{disc} Q = m^2 \operatorname{disc} Q', \quad \gcd(n, m) = 1.$$

*Then, the form $(nQ) * (mQ')$ has primitivity index nm (if the composition exists).*

This result follows from repeating the construction of the composition in this more general setup; the interested reader will find a detailed account in [2, Ch. 1, Sect. 3]. In particular, going back to the case of $Q = dQ_0$ and $Q' = d'Q'_0$, we see that $Q * Q'$ has primitivity index dd' . Also,

$$D = \operatorname{disc}(Q * Q') = (dd')^2 \gcd(f_0, f'_0)^2 d_K,$$

and therefore the primitive part of $Q * Q'$ comes from the order of conductor $\gcd(f_0, f'_0)$.

Under the 1:1 correspondence between the form class group $C(D)$ and the ideal class group $C(\mathcal{O})$ (where \mathcal{O} is the unique order of discriminant D), we see that the form $(1, 1, 1) \in C(-3)$ corresponds to the ideal $[1, \frac{-1+\sqrt{-3}}{2}] \in C(\mathcal{O}_K)$ ($K = \mathbb{Q}(\sqrt{-3})$). But also the form $(3, 3, 3)$ is sent to the same ideal, and therefore we can freely lift a form to larger discriminant without changing the ideal class. This suggests that the extended class group should be redefined as

$$\overline{C}(D) := \bigsqcup_{m|f(D)} C(D/m^2), \quad (\text{drop } m \text{ in all factors})$$

and consequently we define the *extended ideal group*⁴ as

$$\overline{C}(\mathcal{O}) := \bigsqcup_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K} C(\mathcal{O}').$$

The bijection $C(D) \leftrightarrow C(\mathcal{O})$ yields an analogous bijection $\overline{C}(D) \leftrightarrow \overline{C}(\mathcal{O})$; this allows us to work with ideal classes rather than forms.

Fix a quadratic imaginary field K , and let \mathcal{O}_1 (resp. \mathcal{O}_2) be the order of discriminant D_1 (resp. D_2) in \mathcal{O}_K ; let f_1 (resp. f_2) be its conductor and set

$$f_0 := \gcd(f_1, f_2), \quad \bar{f}_1 := f_1/f_0, \quad \bar{f}_2 := f_2/f_0.$$

Composing forms of discriminants D_1 and D_2 gives forms of discriminant $D := \operatorname{lcm}(D_1, D_2)$ ($f := f(D)$), having index of primitivity $d_1 d_2$,

⁴Again, this is not a group!

where $d_1 := f/f_1$ and $d_2 := f/f_2$. Dropping the index we get a composition

$$C(D_1) \times C(D_2) \xrightarrow{\circledast} C(D_0),$$

where $D_0 := f_0^2 d_K$. More concretely, given $Q_1 \in C(D_1)$ and $Q_2 \in C(D_2)$, $Q_1 \circledast Q_2$ is the form in $C(D_0)$ with the property that

$$d_1 d_2 [Q_1 \circledast Q_2] = [d_1 Q_1] * [d_2 Q_2].$$

On the level of ideal classes, we get the usual multiplication between ideals

$$C(\mathcal{O}_{K,f_1}) \times C(\mathcal{O}_{K,f_2}) \rightarrow C(\mathcal{O}_{K,f_0}).$$

We now establish some elementary properties of \circledast (and of $*$ in its original sense).

Proposition 4.2. *Let $Q_i \in C(D_i)$ ($i = 0, 1, 2$), $R \in C(D)$, and let P be the principal form of discriminant D . The composition \circledast satisfies:*

- (i) $[Q_0] \circledast [P] = [Q_0]$;
- (ii) $([Q_0] \circledast [R]) \circledast [R]^{-1} = [Q_0]$;
- (iii) $([Q_1] \circledast [R]) \circledast ([R]^{-1} \circledast [Q_2]) = [Q_1] \circledast [Q_2]$;

Proof. Making use of the isomorphism between form class group and ideal class group, the proof follows easily from the corresponding properties for fractional ideals. \square

4.2. Explicit computation of transcendental lattices. We now exhibit a formula for the transcendental lattice of a singular abelian surface, which is a product of two elliptic curves $E_1 \in \mathcal{E}ll(\mathcal{O}_{K,f_1})$ and $E_2 \in \mathcal{E}ll(\mathcal{O}_{K,f_2})$.

Proposition 4.3. *Let $D_0 = f_0^2 d_K$ and $D'_0 = (f'_0)^2 d_K$, where d_K is the fundamental discriminant of a quadratic imaginary field K . Let $Q_0 = (a_0, b_0, c_0) \in C(D_0)$ and $Q'_0 = (a'_0, b'_0, c'_0) \in C(D'_0)$; if*

$$f := \text{lcm}(f_0, f'_0), \quad d := f/f_0, \quad d' := f/f'_0,$$

consider the forms $Q := dQ_0$ and $Q' := d'Q'_0$ of discriminant $D := f^2 d_K$. Set

$$\tau := \tau(Q_0) = \frac{-b + \sqrt{D}}{2a}, \quad \tau' := \tau(Q'_0) = \frac{-b' + \sqrt{D}}{2a'},$$

where $a = da_0$, $b = db_0$ and $c = dc_0$, and let $E := E_\tau \in \mathcal{E}ll(\mathcal{O}_{K,f_0})$ and $E' := E_{\tau'} \in \mathcal{E}ll(\mathcal{O}_{K,f'_0})$. Then

$$[\mathbf{T}(E \times E')] = [Q] * [Q'] = dd'[Q_0 \circledast Q'_0],$$

where \circledast is the generalized Dirichlet composition.

Proof. The proof is similar to the one of Theorem 3.5; we will just give an outline. By using Dirichlet composition, we can assume that

$$\tau := \frac{-B + \sqrt{D}}{2a}, \quad \tau' := \frac{-B + \sqrt{D}}{2a'},$$

where B is the integer coming into play because of the Dirichlet composition. Computations which are analogous to the ones above yield

$$\mathrm{NS}(A)_{\mathbb{Q}} = \mathbb{Q} \left\langle u^{12} - \frac{B}{a} u^{23} + \frac{D - B^2}{4aa'} u^{34}, u^{14} - \frac{a'}{a} u^{23}, u^{13}, u^{24} \right\rangle.$$

The transcendental lattice $\mathrm{T}(A)$ is given by the conditions

$$A_{24} = A_{13} = 0, \tag{5}$$

$$A_{34} - \frac{B}{a} A_{14} + \frac{D - B^2}{4aa'} A_{12} = 0, \tag{6}$$

$$A_{23} - \frac{a'}{a} A_{14} = 0. \tag{7}$$

Condition (7) gives

$$da_0 A_{23} = d'a'_0 A_{14};$$

now we can assume that $(d, a'_0) = 1$ and then also that $(a_0, a') = 1$. Under these assumptions, we see that

$$A_{14} = a_0 A'_{14} = a_0 d A''_{14} \quad \text{and} \quad A_{23} = a'_0 d' A''_{14};$$

substituting in (6) yields

$$A_{34} = B A''_{14} + C A_{12},$$

and therefore we deduce

$$\mathrm{T}(A) = \mathbb{Z} \left\langle au^{14} + a'u^{23} + Bu^{34}, u^{12} + Cu^{34} \right\rangle = \begin{pmatrix} 2aa' & B \\ B & 2C \end{pmatrix}.$$

□

Example 4.4 (Example 3.7 continued). We can now get all decompositions of the abelian surface A having transcendental lattice $\mathrm{T}(A) = 6(1, 0, 3)$. In fact, since $h(\mathcal{O}_{K,2}) = 1$, any pair of elliptic curves (E_1, E_2) with $E_1 \in \mathcal{E}ll(\mathcal{O}_{K,4})$ and $E_2 \in \mathcal{E}ll(\mathcal{O}_{K,3})$ gives a decomposition; also, we can use pairs (E_1, E_2) with $E_1 \in \mathcal{E}ll(\mathcal{O}_{K,2})$ and $E_2 \in \mathcal{E}ll(\mathcal{O}_{K,12})$. It is easy to verify that we get exactly 24 strict decompositions.

4.3. New candidate decompositions. As a consequence of Proposition 4.3, we get a new family of decompositions of a given abelian surface A of transcendental lattice $Q = nQ_0$. Indeed, the group $C(D)$ acts on the class groups $C(D_1)$ and $C(D_2)$ by \circledast , and therefore, once we are given a decomposition $A = E_{\tau(Q_1)} \times E_{\tau(Q_2)}$, we get new ones by taking

$$E_{\tau([Q_1] \circledast [R])} \times E_{\tau([Q_2] \circledast [R]^{-1})}, \quad [R] \in C(D).$$

Notice that we can always cook up such a decomposition: consider the forms Q_0 and P_0 (the latter being the principal form) of discriminant D_0 , and if $s, t \in \mathbb{Z}$ are coprime nonnegative integers consider the abelian surface $E_{s\tau(Q_0)} \times E_{t\tau(P_0)}$ as in Theorem 3.5. Then, it gives indeed a decomposition of A ; now notice that $s\tau(Q_0)$ corresponds to the form

$$ax^2 + (bs)xy + (cs^2)y^2,$$

which is primitive in $C(s^2D)$, and similar considerations hold for $t\tau(P_0)$.

Now that we have these families of decompositions, is there a way of getting them all? Namely, to what extent does the action of $C(D)$ on $C(D_1)$ and $C(D_2)$ give a description of the possible decompositions?

5. DECOMPOSITIONS IN THE CASES $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$

5.1. Action of a class group on class groups of smaller discriminant. Recall that if $D_0|D$, the class group $C(D)$ acts on $C(D_0)$. Therefore, we might ask whether the action is transitive. Notice that a form $Q_0 \in C(D_0)$ can be lifted to a primitive form $Q \in C(D)$ in such a way that $Q \circledast P_0 = Q_0$.

Lemma 5.1. *For every form $Q_0 \in C(D_0)$ there exists a form $Q \in C(D)$ which is the lift of Q_0 in the following sense: $Q \circledast P_0 = Q_0$.*

Proof. If $Q_0 = [a_0, b_0, c_0]$ is represented by the ideal $[a_0, \frac{-b_0+\sqrt{D_0}}{2}]$, then Q correspond to the ideal $[a_0, \frac{-db_0+\sqrt{D}}{2}]$; also $dP_0 = [d, \frac{-dp_0+\sqrt{D}}{2}]$, where $p_0 = 0, 1$ according to the parity of the discriminant D . It follows that

$$[Q] * [dP_0] = [a_0d, \Delta] = [a_0, \Delta/d] = [Q],$$

where $\Delta = \frac{-B+\sqrt{D}}{2}$, and B is the usual key integer in the Dirichlet composition. \square

As a consequence, we have the following

Corollary 5.2. *The action of $C(D)$ on $C(D_0)$ is transitive.*

This means that the factors of the decompositions

$$E_{\tau([Q_1] \circledast [R])} \times E_{\tau([Q_2] \circledast [R]^{-1})}, \quad [R] \in C(D)$$

cover the whole class groups $C(D_1)$ and $C(D_2)$. However, we do not know whether we get distinct decompositions under this action. Of course, if this were the case, then we would obtain the whole set of decompositions, matching Ma's formula.

5.2. Distinct decompositions. We now come to the issue of whether the set of decompositions we get with the above technique is complete or not. To do so, let us assume $Q_1 \in C(D_1)$, $Q_2 \in C(D_2)$ and $R, S \in C(D)$. Moreover, suppose that

$$[Q_1] \circledast [R] = [Q_1] \circledast [S], \quad [Q_2] \circledast [R]^{-1} = [Q_2] \circledast [S]^{-1},$$

which is the case of a decomposition being realized by two elements $R, S \in C(D)$. This is equivalent to the existence of an element $U \in C(D)$ such that

$$U \circledast Q_1 = Q_1, \quad U \circledast Q_2 = Q_2.$$

So we are to understand the elements $U \in C(D)$ that fix Q_i , $i = 1, 2$.

Let $C(D)$ act on $C(D_0)$, and let U be an element fixing some $Q_0 \in C(D_0)$; notice that U would actually fix the whole class groups $C(D_0)$. We call the group of such U 's the *stabilizer* of $C(D_0)$ in $C(D)$, and it will be denoted by $\text{Stab } C(D_0)$; clearly, its order is $h(D)/h(D_0)$. In the situation of interest to us, we can consider the intersection $\text{Stab } C(D_1) \cap \text{Stab } C(D_2)$: it describes the elements in $C(D)$ that represent an obstruction to having the full set of decompositions by twisting by $C(D)$ the factors of a given decomposition.

It may occur that $\text{Stab } C(D_1) \cap \text{Stab } C(D_2)$ is trivial, for instance when the class number or the index of primitivity are small enough, or even when the orders of the stabilizers are powers of different primes. However, it is not difficult to come up with an example of this not being the case when $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$.

Example 5.3. Let $Q = 30 \cdot (1, 0, 3) \in \overline{C}(D)$, where $D = -60^2 3$. If A is the singular abelian surface with $T(A) = Q$, then we know by Corollary 3.1 that $\tilde{\delta}(A) = 288$. There are four classes of products we have to consider.

- (1) $\mathcal{Ell}(\mathcal{O}_{K,2}) \times \mathcal{Ell}(\mathcal{O}_{K,60})$: we already noticed above that this class gives $2h(\mathcal{O}_{K,60}) = 72$ distinct strict decompositions.

- (2) $\mathcal{E}ll(\mathcal{O}_{K,4}) \times \mathcal{E}ll(\mathcal{O}_{K,30})$: we need to estimate the order of the stabilizers. We have (by means of the class number formula)

$$\#\text{Stab } C(\mathcal{O}_{K,4}) = h(\mathcal{O}_{K,60})/h(\mathcal{O}_{K,4}) = 18,$$

$$\#\text{Stab } C(\mathcal{O}_{K,30}) = h(\mathcal{O}_{K,60})/h(\mathcal{O}_{K,30}) = 2.$$

It follows that $\#(\text{Stab } C(\mathcal{O}_{K,4}) \cap \text{Stab } C(\mathcal{O}_{K,30})) \leq 2$, and thus we get at least $h(\mathcal{O}_{K,60}) = 36$ distinct strict decompositions.

- (3) $\mathcal{E}ll(\mathcal{O}_{K,6}) \times \mathcal{E}ll(\mathcal{O}_{K,20})$: by using the class number formula, we see that

$$\#\text{Stab } C(\mathcal{O}_{K,6}) = h(\mathcal{O}_{K,60})/h(\mathcal{O}_{K,6}) = 12,$$

$$\#\text{Stab } C(\mathcal{O}_{K,20}) = h(\mathcal{O}_{K,60})/h(\mathcal{O}_{K,20}) = 3;$$

thus $\#(\text{Stab } C(\mathcal{O}_{K,6}) \cap \text{Stab } C(\mathcal{O}_{K,20})) \leq 3$, and we get at least $2h(\mathcal{O}_{K,60})/3 = 24$ distinct strict decompositions.

- (4) $\mathcal{E}ll(\mathcal{O}_{K,10}) \times \mathcal{E}ll(\mathcal{O}_{K,10})$: by using the class number formula, we see that

$$\#\text{Stab } C(\mathcal{O}_{K,10}) = h(\mathcal{O}_{K,60})/h(\mathcal{O}_{K,10}) = 6,$$

$$\#\text{Stab } C(\mathcal{O}_{K,12}) = h(\mathcal{O}_{K,60})/h(\mathcal{O}_{K,12}) = 6;$$

thus $\#(\text{Stab } C(\mathcal{O}_{K,10}) \cap \text{Stab } C(\mathcal{O}_{K,12})) \leq 6$, and we get at least $2h(\mathcal{O}_{K,60})/6 = 12$ distinct strict decompositions.

In total, we have obtained at least 144 distinct decompositions out of 288.

The question we would like to answer is the following

Question 5.4. Is $\text{Stab } C(\mathcal{O}_{K,f_1}) \cap \text{Stab } C(\mathcal{O}_{K,f_2})$ is always trivial, or at least when $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$?

Indeed, this will be the case, as we are going to show in the following.

5.3. Answer to the question. The key ingredient is the fact that the principal form represents all but finitely many unramified primes which split completely in the ring class field. Let P_i be the principal form of the order \mathcal{O}_{K,f_i} , $i = 1, 2, \emptyset$. Also, let L_i be the ring class field of the order \mathcal{O}_{K,f_i} , $i = 1, 2, \emptyset$.

Lemma 5.5. *Let \mathcal{P}_{P_i} be the set of primes of represented by P_i , for $i = 1, 2, \emptyset$. Then, $\mathcal{P}_P \doteq \mathcal{P}_{P_1} \cap \mathcal{P}_{P_2}$.*

Proof. By using Lemma 2.6, we see that

$$\mathcal{P}_P \doteq \text{Spl}(L/K) = \text{Spl}(L_1/K) \cap \text{Spl}(L_2/K) \doteq \mathcal{P}_{P_1} \cap \mathcal{P}_{P_2}.$$

□

By the Čebotarev Density Theorem, we can reason with the set \mathcal{P}_{P_i} rather than $\text{Spl}(L_i/K)$, for $i = 1, 2, \emptyset$: in fact, they both have positive Dirichlet density (thus they are infinite), and they are the same up to a finite set (which has Dirichlet density 0).

Proposition 5.6. *The principal form is characterized by representing almost all primes that split completely in the ring class field.*

Proof. Suppose Q is a form such that $\mathcal{P}_Q \doteq \text{Spl}(L/K)$. Then, we would have

$$\left\{ p \text{ prime} \mid p \text{ unramified}, \left(\frac{L/K}{p}\right) = \langle \sigma \rangle \right\} \doteq \left\{ p \text{ prime} \mid \left(\frac{L/K}{p}\right) = \langle 1 \rangle \right\},$$

and since both sets have infinitely many elements it must necessarily be $\sigma = 1 \in \text{Gal}(L/K)$, which corresponds to the class of the principal form. Since equivalent forms represent the same numbers, we are done. \square

We can now answer Question 5.4:

Theorem 5.7. *Unless $d_K \in \{-3, -4\}$, $f_1, f_2 > 1$ and $f_0 = 1$, we have*

$$\text{Stab } C(\mathcal{O}_{K,f_1}) \cap \text{Stab } C(\mathcal{O}_{K,f_2}) = (0).$$

Proof. Let $[Q] \in \text{Stab } C(D_1) \cap \text{Stab } C(D_2)$, i.e. $[Q]$ is such that

$$Q \circledast P_1 = P_1, \quad Q \circledast P_2 = P_2.$$

Now, for $i = 1, 2$, the primes represented by P_i are, up to a finite set, those p that split completely in the ring class field L_i . In the same fashion, the primes represented by Q are, up to a finite set, the ones splitting completely in the ring class field L . Notice that, by the assumption, it follows that all primes represented by Q are also represented by P_1 and P_2 . Moreover, by Proposition 2.5, $L = L_1 L_2$, and Lemma 5.5 and Proposition 5.6 imply that Q is in fact the principal form. \square

Now, let us recall that to an element $[Q] \in C(\mathcal{O})$ in a class group we can associate an elliptic curve by setting $E_Q := E_{\tau(Q)}$. In light of this, we can rephrase the previous result as follows.

Theorem 5.8. *Unless $d_K \in \{-3, -4\}$, $f_1, f_2 > 1$ and $f_0 = 1$, the group $C(\mathcal{O}_{K,f})$ spans all the possible decompositions of A into the products of elliptic curves with classes in $C(\mathcal{O}_{K,f_1})$ and $C(\mathcal{O}_{K,f_2})$.*

As a consequence, we obtain the classification theorem for decompositions of singular abelian surfaces in case the transcendental lattice is not a multiple of $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ or $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

Theorem 5.9. *Let A be a singular abelian surface having transcendental lattice $Q = nQ_0$, with Q_0 neither $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ nor $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$; let $D = f^2 d_K = \text{disc } Q$, $D_0 = f_0^2 d_K = \text{disc } Q_0$ and consider all pairs (f_1, f_2) of positive integer such that*

$$\gcd(f_1, f_2) = f_0 \quad \text{and} \quad f_1 f_2 = n f_0^2.$$

Then A decomposes into the product of two mutually isogenous elliptic curves with complex multiplication according to one of the following possibilities:

- (1) $A \cong E_{\tau([Q_0] \oplus [R])} \times E_{\tau([P] \oplus [R]^{-1})}$, for $[R] \in C(D)$;
- (2) for any choice of a pair (f_1, f_2) such that

$$\gcd(f_1, f_2) = 1 \quad \text{and} \quad f_1 f_2 = n f_0,$$

take a form in the class $[Q_0]$ that lifts to a primitive form Q_1 of discriminant D_1 , and similarly lift a form in $[P_0]$ to a primitive form Q_2 of discriminant D_2 ; then, $A \cong E_{\tau([Q_1] \oplus [R])} \times E_{\tau([Q_2] \oplus [R]^{-1})}$, for $[R] \in C(D)$.

Proof of Theorem 5.9. The result follows by applying Theorem 5.7 to each pair (f_1, f_2) such that

$$f_1 f_2 = n f_0^2 \quad \text{and} \quad \gcd(f_1, f_2) = f_0,$$

and by noticing that the number of decompositions we get matches with Ma's original formula. \square

5.4. Alternative proof of Ma's formula. The classification of decompositions of singular abelian surfaces has been obtained by producing enough distinct decompositions to match Ma's formula. However, our construction incidentally provides the reader with an alternative and simpler proof of the same result, at least in the cases covered by the classification theorem (Theorem 5.7).

Let $\Sigma^{\text{Ab}}(D, n)$ be the space of singular abelian surfaces of discriminant D and primitivity index n , i.e. the space of surfaces A such that $T(A) = nQ_0$, for a primitive form Q_0 , and $\text{disc } T(A) = D$. If we consider all the elements of $\Sigma^{\text{Ab}}(D, n)$ at once, we have constructed a total of

$$2^{\tau(n)} h(\mathcal{O}_{K, f_0}) h(\mathcal{O}_{K, f})$$

distinct product surfaces. However, the number of distinct product surfaces within $\Sigma^{\text{Ab}}(D, n)$ is

$$\sum_{A \in \Sigma^{\text{Ab}}(D, n)} \widetilde{\delta(A)} = \sum_{\substack{(f_1, f_2) = f_0 \\ f_1 f_2 = n f_0^2}} h(\mathcal{O}_{K, f_1}) h(\mathcal{O}_{K, f_2}).$$

We now show that these two numbers are indeed the same; therefore, this result yields a different proof of Ma's formula in most cases.

Proposition 5.10. *Unless $d_K \in \{-3, -4\}$ and $f_0 = 1$, we have*

$$2^{\tau(n)} h(\mathcal{O}_{K, f}) h(\mathcal{O}_{K, f_0}) = \sum_{\substack{(f_1, f_2) = f_0 \\ f_1 f_2 = n f_0^2}} h(\mathcal{O}_{K, f_1}) h(\mathcal{O}_{K, f_2}).$$

Proof. We notice that

$$\begin{aligned} \sum_{\substack{(f_1, f_2) = f_0 \\ f_1 f_2 = n f_0^2}} h(\mathcal{O}_{K, f_1}) h(\mathcal{O}_{K, f_2}) &= 2 \sum_{\substack{(f_1, f_2) = f_0 \\ f_1 f_2 = n f_0^2 \\ f_1 < f_2}} h(\mathcal{O}_{K, f_1}) h(\mathcal{O}_{K, f_2}) \\ &= 2 \sum_{\substack{(f_1, f_2) = f_0 \\ f_1 f_2 = n f_0^2 \\ f_0 \neq f_1 < f_2}} h(\mathcal{O}_{K, f_1}) h(\mathcal{O}_{K, f_2}) + 2h(\mathcal{O}_{K, f_0}) h(\mathcal{O}_{K, f}), \end{aligned}$$

and so it is enough to prove that

$$(2^{\tau(n)-1} - 1) h(\mathcal{O}_{K, f}) = \sum_{\substack{(f_1, f_2) = f_0 \\ f_1 f_2 = n f_0^2 \\ 1 \neq f_1 < f_2}} \frac{h(\mathcal{O}_{K, f_1}) h(\mathcal{O}_{K, f_2})}{h(\mathcal{O}_{K, f_0})};$$

since the number of summands on the right-hand side is precisely $2^{\tau(n)-1} - 1$, we are left to prove that

$$\frac{h(\mathcal{O}_{K, f_1}) h(\mathcal{O}_{K, f_2})}{h(\mathcal{O}_{K, f_0})} = h(\mathcal{O}_{K, f}).$$

But this is a consequence of the class number formula and some easy arithmetic: in fact, by the assumptions,

$$[\mathcal{O}_K^\times : \mathcal{O}_{K, f_i}^\times] = \#\mathcal{O}_K^\times, \quad i = 0, 1, 2.$$

Setting

$$\Pi_i := \prod_{p|f_i} \left(1 - \left(\frac{d_K}{p} \right) \frac{1}{p} \right), \quad i = 0, 1, 2, \emptyset$$

Theorem 2.3 yields

$$\frac{h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2})}{h(\mathcal{O}_{K,f_0})} = \frac{h(\mathcal{O}_K)f_1f_2\Pi_1\Pi_2}{f_0\Pi_0\#\mathcal{O}_K^\times} = \frac{h(\mathcal{O}_K)f}{\#\mathcal{O}_K^\times} \cdot \frac{\Pi_1\Pi_2}{\Pi_0},$$

since $f = nf_0$ and $f_1f_2 = nf_0^2 = ff_0$. However, it is straightforward to see that

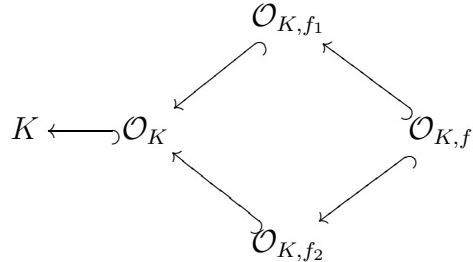
$$\frac{\Pi_1\Pi_2}{\Pi_0} = \Pi,$$

and therefore the proof is complete. \square

6. DECOMPOSITIONS IN THE REMAINING CASES

6.1. Number of decompositions and classification. Unfortunately, the techniques employed thus far cannot be employed when $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$, as we might have nontrivial elements in $\text{Stab } C(\mathcal{O}_{K,f_1}) \cap \text{Stab } C(\mathcal{O}_{K,f_2})$. However, we are still able to completely solve the classification problem. First of all, we would like to point out that a formula for the number of decompositions in these two cases can be obtained just by counting, as the class number of \mathcal{O}_K is one.

Assume first that $K = \mathbb{Q}(i)$ and that we are given a singular abelian surface A with transcendental lattice $\begin{pmatrix} 2n & 0 \\ 0 & 2n \end{pmatrix}$; then, we have the following diagram,



where f_1 and f_2 are relatively prime, and actually $f = n$.

Theorem 6.1. *Given a singular abelian surface A with transcendental lattice $\begin{pmatrix} 2n & 0 \\ 0 & 2n \end{pmatrix}$, the number of decompositions of A into the product of two mutually isogenous elliptic curves with complex multiplication (up to isomorphism of the factors) is*

$$\tilde{\delta}(A) = (1 + 2^{\tau(n)-1})h(\mathcal{O}_{K,n}).$$

The surface A is isomorphic to any of the products (E_1, E_2) , where $[E_i] \in \mathcal{E}\ell\ell(\mathcal{O}_{K,f_i})$ ($i = 1, 2$), $\gcd(f_1, f_2) = 1$ and $f_1f_2 = n$.

Proof. Since $h(\mathcal{O}_K) = 1$, we see that

$$\begin{aligned}\tilde{\delta}(A) &= \sum_{\substack{(f_1, f_2)=1 \\ f_1 f_2=n}} h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2}) = 2 \sum_{\substack{(f_1, f_2)=1 \\ f_1 f_2=n \\ f_1 < f_2}} h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2}) \\ &= 2 \sum_{\substack{(f_1, f_2)=1 \\ f_1 f_2=n \\ 1 \neq f_1 < f_2}} h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2}) + 2h(\mathcal{O}_{K,n}).\end{aligned}$$

Following the notation from earlier, since $\#\mathcal{O}_K^\times = 4$, the class number formula implies that $h(\mathcal{O}_{K,f_i}) = f_i \Pi_i / 2$. Therefore, $h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2}) = n \Pi / 4$, and thus

$$\begin{aligned}\tilde{\delta}(A) &= (2^{\tau(n)-1} - 1)n\Pi/2 + n\Pi \\ &= \frac{1}{2}n\Pi(1 + 2^{\tau(n)-1}) = (1 + 2^{\tau(n)-1})h(\mathcal{O}_{K,n}).\end{aligned}$$

So we are able to exhibit a formula for the number of decompositions of such a singular abelian surface. Also, the classification problem is solved, as we can just take all pairs (E_1, E_2) fitting in the diagram above. \square

The case $K = \mathbb{Q}(\sqrt{-3})$ is analogous, and thus the proof of Theorem 6.2 is the same, except for the fact that $\#\mathcal{O}_K^\times = 6$.

Theorem 6.2. *Given a singular abelian surface A with transcendental lattice $\begin{pmatrix} 2n & n \\ n & 2n \end{pmatrix}$, the number of decompositions of A into the product of two mutually isogenous elliptic curves with complex multiplication (up to isomorphism of the factors) is*

$$\tilde{\delta}(A) = \frac{2}{3}(2 + 2^{\tau(n)-1})h(\mathcal{O}_{K,n}).$$

The surface A is isomorphic to any of the products (E_1, E_2) , where $[E_i] \in \mathcal{E}ll(\mathcal{O}_{K,f_i})$ ($i = 1, 2$), $\gcd(f_1, f_2) = 1$ and $f_1 f_2 = n$.

Although the counting and the classification problems are completely solved, it is not clear whether the action of the class group $C(\mathcal{O}_{K,f})$ spans the set of decompositions of A .

6.2. Application: Shioda-Inose models of singular K3 surfaces. Let X be a singular K3 surface, and let $T(X)$ denote its transcendental lattice. By results of Shioda and Inose [9], there exists a singular abelian surface $A = E_1 \times E_2$ such that $T(A) = T(X)$; moreover, there

is a model of X which is given in terms of the j -invariants of E_1 and E_2 . In [7], the author gives a very nice model for such a K3 surface, namely X has the following model as an elliptic fibration

$$X : \quad y^2 = x^3 - 3ABt^4x + ABt^5(Bt^2 - 2Bt + 1),$$

where $A = j_1j_2$ and $B = (1 - j_1)(1 - j_2)$, j_k being the j -invariant of E_k ($k = 1, 2$). It follows that our classification of the decompositions of a singular abelian surface gives all the possible Shioda-Inose models of X , i.e. all the possible models of X which are realizable via a Shioda-Inose structure.

6.3. Application: fields of moduli of singular K3 surfaces. We now provide an application of our results to the theory of singular K3 surfaces. It is well-known that every singular abelian surface yields a singular K3 surface by means of a Shioda-Inose structure [9]. We are interested in some arithmetic invariant of the latter, namely the field of moduli. We recall that M is the (absolute) *field of moduli* of a variety X over a number field if for all automorphisms $\sigma \in \text{Aut}(\mathbb{C}/\mathbb{Q})$,

$$X^\sigma \in [X] \iff \sigma \text{ acts trivially on } M,$$

where by $[X]$ we denote the isomorphism class of X . The field of moduli exists and is unique, since by Galois theory it is equivalently defined as the fixed field of the group

$$G := \{\sigma \in \text{Aut}(\mathbb{C}/\mathbb{Q}) \mid X^\sigma \in [X]\}.$$

Generalizing a previous result of Shimada [8], Schütt was able to prove the following result

Theorem 6.3 (Theorem 5.2 in [7]). *Let X be a singular K3 surface, and let $T(X)$ be its transcendental lattice. Assume that X is defined over a Galois extension L/K , where $K = \mathbb{Q}(\text{disc } T(A))$. Then, the action of the Galois group $\text{Gal}(L/K)$ spans the genus of $T(X)$, i.e.*

$$(\text{genus of } T(X)) = \{[T(X^\sigma)] \mid \sigma \in \text{Gal}(L/K)\}.$$

Set $L := H(\text{disc } T(X))$ in the statement above, where $H(D)$ denotes the ring class field of the order in K of discriminant D , for $D < 0$. Class field theory tells us that

$$\text{Gal}(L/\mathbb{Q}) \cong \text{Gal}(L/K) \rtimes \text{Gal}(K/\mathbb{Q}),$$

where $\text{Gal}(K/\mathbb{Q})$ accounts for the complex conjugation (for a reference, see [2, Ch. 9]). But complex conjugation has the effect of sending a singular K3 surface of transcendental lattice $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ to the singular

K3 surface with transcendental lattice $\begin{pmatrix} 2a & -b \\ -b & 2c \end{pmatrix}$, so it acts as inversion on the corresponding class group (see [10] and [7]). By observing that a form and its inverse lie in the same genus, we conclude that

$$\begin{aligned} (\text{genus of } T(X)) &= \{[T(X^\sigma)] \mid \sigma \in \text{Gal}(L/K)\} = \\ &= \{[T(X^\sigma)] \mid \sigma \in \text{Gal}(L/\mathbb{Q})\}. \end{aligned}$$

This suggests a connection between the field of moduli of a singular K3 surface and the genus of its transcendental lattice. In fact, the problem of characterizing the field of moduli of singular K3 surfaces is dealt with in a paper of the author [4].

The classification of decompositions of a singular abelian surface allows us to tell something more about the field of moduli of X . Recall that M is contained in the intersection of all possible fields of definition. Then, by means of a Shioda-Inose structure starting from a suitable singular abelian surface $E_1 \times E_2$, X admits a model over $\mathbb{Q}(j_1 j_2, j_1 + j_2)$ by a result of Schütt [7]. Therefore, considering all admissible pairs (E_1, E_2) such that $T(E_1 \times E_2) = T(X)$, we see that

$$M \subseteq \bigcap_{X \text{ defined over } L} L \subseteq \bigcap_{j_1, j_2 \text{ as above}} \mathbb{Q}(j_1 j_2, j_1 + j_2).$$

We deduce a slightly clearer picture of what M looks like, as we know where it has to sit as an extension of \mathbb{Q} . Namely, M lies in right-hand side above, which is not hard to describe theoretically. In practice, describing it is a hard task, as this involves the computation of several j -invariants.

6.4. Open problems. The present treatment deals with decompositions of singular abelian surfaces, but one might want to investigate the possible decompositions in the case of singular abelian varieties of higher dimension. It was proven by Katsura [3] that such a variety is isomorphic to the product of mutually isogenous elliptic curves with CM.

Problem 6.4. Given a singular abelian variety A , how many decompositions of A into the product of mutually isogenous elliptic curves are there? What are the possible decompositions?

REFERENCES

- [1] B. Allombert, Y. Bilu, and A. Pizarro-Madariaga. CM-Points on Straight Lines. arXiv:1406.1274, June 2014.

- [2] D. A. Cox. *Primes of the form $x^2 + ny^2$* . Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.
- [3] T. Katsura. On the structure of singular abelian varieties. *Proc. Japan Acad.*, 51(4):224–228, 1975.
- [4] R. Laface. The field of moduli of singular abelian and K3 surfaces. *ArXiv e-prints*, January 2016.
- [5] S. Ma. Decompositions of an Abelian surface and quadratic forms. *Ann. Inst. Fourier (Grenoble)*, 61(2):717–743, 2011.
- [6] D.R. Morrison. On K3 surfaces with large Picard number. *Inventiones mathematicae*, 75(1):105–121, 1984.
- [7] M. Schütt. Fields of definition of singular K3 surfaces. *Commun. Number Theory Phys.*, 1(2):307–321, 2007.
- [8] I. Shimada. Transcendental lattices and supersingular reduction lattices of a singular K3 surface. *Trans. Amer. Math. Soc.*, 361(2):909–949, 2009.
- [9] T. Shioda and H. Inose. On singular K3 surfaces. In *Complex analysis and algebraic geometry*, pages 119–136. Iwanami Shoten, Tokyo, 1977.
- [10] T. Shioda and N. Mitani. Singular abelian surfaces and binary quadratic forms. In *Classification of algebraic varieties and compact complex manifolds*, pages 259–287. Lecture Notes in Math., Vol. 412. Springer, Berlin, 1974.

INSTITUT FÜR ALGEBRAISCHE GEOMETRIE, GOTTFRIED LEIBNIZ UNIVERSITÄT HANNOVER, WELFENGARTEN 1 30167 HANNOVER (GERMANY)

E-mail address: laface@math.uni-hannover.de